

# Two families of planar functions on $\mathbb{F}_{p^{2r}}$

Stephen M. Gagola III · Joanne L. Hall

Received: date / Accepted: date

**Abstract** Two new families of planar functions are constructed. These new families are part of a more general construction which also includes a family of planar functions recently constructed by Bierbrauer [Commutative semifields from projection mappings, *Designs, Codes and Cryptography*, **61** (2011), 187–196].

**Keywords** Projective plane · Planar function · Dembowski-Ostrom polynomial · Semifield · Trace

**Mathematics Subject Classification (2010)** MSC 51E15 · 05B25 · 51A40 · 94A60

## 1 Introduction

Planar functions belong to the larger class of highly nonlinear functions which are of use in classical cryptographic systems, quantum cryptographic systems [19], wireless communication signals [12], coding theory [15] as well as being of theoretical interest [7] [9].

Let  $\mathbb{F}_{p^r}$  be a field of characteristic  $p$ . A function  $f : \mathbb{F}_{p^r} \rightarrow \mathbb{F}_{p^r}$  is called a *planar function* if for every  $a \in \mathbb{F}_{p^r}^*$  the function  $\Delta_{f,a} : x \mapsto f(x+a) - f(x)$  is a bijection.

Recent and extensive lists of planar functions can be found in [18, 4].

---

S.M. Gagola III (corresponding Author), J.L. Hall  
Department of Algebra  
Charles University  
Tel.: +420 22191 3238  
Fax: +420 22232 3386  
E-mail: gagola@karlin.mff.cuni.cz

J.L. Hall  
School of Mathematical Sciences  
Queensland University of Technology

The main result of this paper is two new planar functions.

**Theorem 1** *Let  $g(x), h(x) \in \mathbb{F}_{p^{2r}}[x]$ , with  $g(x) = x^2$  and  $h(x) = x^{p^i + p^k}$  where  $0 \leq i < k < 2r$ . If  $h(x)$  is planar over  $\mathbb{F}_{p^{2r}}$  then*

$$(1) \quad f_1(x) = g(x) + (g(x))^{p^r} + h(x) - (h(x))^{p^r}$$

and

$$(2) \quad f_2(x) = h(x) + (h(x))^{p^r} + g(x) - (g(x))^{p^r}$$

are planar functions. Furthermore,  $f_1(x)$  and  $f_2(x)$  are not CCZ-equivalent.

The planar functions of Theorem 1 belong to a more general class which also contains a recently published family of planar functions by Bierbrauer. Section 2 contains this general construction. Section 3 provides the proof of Theorem 1, showing that the families  $f_1$  and  $f_2$  are nonequivalent planar functions. In section 4 it is demonstrated that the families  $f_1$  and  $f_2$  are new, with nonequivalence to all known planar functions demonstrated. Section 5 contains some nonexistence results when searching for more planar functions that meet the general construction of section 2.

## 2 General construction

There are 14 known distinct families of planar functions. A look at a recent list of planar functions [4] shows no obvious pattern. Computational searches can discover new planar functions [16], but algebraic work is required to significantly deepen our understanding. A computational search for planar functions was performed on small fields. Several new functions were found that fit the shape of Theorem 2, leading to this general result.

**Theorem 2** *Let  $p$  be an odd prime and let  $g(x)$  and  $h(x)$  be functions on  $\mathbb{F}_{p^{2r}}$ . Let*

$$f(x) = g(x) + (g(x))^{p^r} + h(x) - (h(x))^{p^r}, \quad (1)$$

then  $f(x)$  is a planar function if and only if for any  $x \in \mathbb{F}_{p^{2r}}$  and  $a, b \in \mathbb{F}_{p^{2r}}^*$

$$\Delta_{\Delta_{g,a},b}(x) + (\Delta_{\Delta_{g,a},b}(x))^{p^r} = 0$$

implies that  $\Delta_{\Delta_{h,a},b}(x) \notin \mathbb{F}_{p^r}$ .

**Observation 3**  $f(x)$  is planar if and only if

$$\Delta_{\Delta_{f,a},b} = \Delta_{f,a}(x+b) - \Delta_{f,a}(x) \neq 0 \quad \text{for all } x, a, b \in \mathbb{F}_{p^{2r}}, \text{ with } a, b \neq 0.$$

*Proof* Since  $\mathbb{F}_{p^r}$  is a subfield of  $\mathbb{F}_{p^{2r}}$ , the trace function

$$Tr(x) = Tr_{\mathbb{F}_{p^{2r}}/\mathbb{F}_{p^r}}(x) = x + x^{p^r}$$

can be used in rewriting  $f(x)$ :

$$f(x) = Tr(g(x)) + h(x) - (h(x))^{p^r}.$$

Then, from Observation 3,  $f(x)$  is planar if and only if

$$\Delta_{\Delta_{f,a},b}(x) = Tr(\Delta_{\Delta_{g,a},b}(x)) + \Delta_{\Delta_{h,a},b}(x) - (\Delta_{\Delta_{h,a},b}(x))^{p^r} \neq 0$$

for all  $x \in \mathbb{F}_{p^{2r}}$  and  $a, b \in \mathbb{F}_{p^{2r}}^*$ .

Now assume that  $\Delta_{\Delta_{f,a},b}(x) = 0$ . Then

$$Tr(\Delta_{\Delta_{g,a},b}(x)) + \Delta_{\Delta_{h,a},b}(x) - (\Delta_{\Delta_{h,a},b}(x))^{p^r} = 0 \quad (2)$$

$$\implies \left( Tr(\Delta_{\Delta_{g,a},b}(x)) + \Delta_{\Delta_{h,a},b}(x) - (\Delta_{\Delta_{h,a},b}(x))^{p^r} \right)^{p^r} = 0 \quad (3)$$

$$\implies Tr(\Delta_{\Delta_{g,a},b}(x)) + (\Delta_{\Delta_{h,a},b}(x))^{p^r} - \Delta_{\Delta_{h,a},b}(x) = 0. \quad (4)$$

By adding Equations (2) and (4) it follows that  $\Delta_{\Delta_{f,a},b} = 0$  if and only if

$$Tr(\Delta_{\Delta_{g,a},b}(x)) = 0 \quad \text{and} \quad (5)$$

$$\Delta_{\Delta_{h,a},b}(x) - (\Delta_{\Delta_{h,a},b}(x))^{p^r} = 0. \quad (6)$$

Thus  $f(x)$  is planar if and only if for any  $x \in \mathbb{F}_{p^{2r}}$  and  $a, b \in \mathbb{F}_{p^{2r}}^*$  either Equation (5) or Equation (6) does not hold. Note that Equation (6) holds exactly when  $\Delta_{\Delta_{h,a},b}(x) \in \mathbb{F}_{p^r} \subset \mathbb{F}_{p^{2r}}$ . Hence,  $f(x)$  is planar if and only if for any  $x \in \mathbb{F}_{p^{2r}}$  and  $a, b \in \mathbb{F}_{p^{2r}}^*$

$$Tr(\Delta_{\Delta_{g,a},b}(x)) = 0$$

implies that  $\Delta_{\Delta_{h,a},b}(x) \notin \mathbb{F}_{p^r}$ .

Theorem 2 has established necessary and sufficient conditions for the seed functions  $g(x), h(x)$  to form a planar function using Equation (1). There is a family of planar functions already known that fits the shape of Theorem 2.

**Theorem 4** [2, Thm 1] Let  $g(x) = \frac{1}{2}x^2$  and

$$h(x) = \frac{1}{2} \sum_{i=0}^k (-1)^i x^{(1+p^2)p^{2i}} + \frac{1}{2} \sum_{j=0}^{k-1} (-1)^{k+j} x^{(1+p^2)p^{2j+1}} \quad (7)$$

Then the function  $f(x)$  defined in Theorem 2 is a planar function on  $\mathbb{F}_{p^{2(2k+1)}}$  for  $k > 0$ .

Some new functions meeting the conditions are presented in Theorem 1 and proved in the next section.

A polynomial  $f(x) \in \mathbb{F}_{p^r}[x]$  is a *Dembowski-Ostrom* polynomial [9] if its reduced form has the shape

$$f(x) = \sum_{i,j=0}^k a_i x^{p^i + p^j}. \quad (8)$$

Any polynomial  $f(x) \in \mathbb{F}_{p^r}[x]$  may be *reduced* modulo  $x^{p^r} - x$ , which yields a polynomial of degree less than  $p^r$  that induces the same function on  $\mathbb{F}_{p^r}$  [9]. All but one known family of planar functions are DO polynomials [18]. Note that the seed functions, and hence the planar function in Theorem 4 are all DO polynomials. Henceforth focus is on seed functions which are DO polynomials.

Notions of equivalence of polynomials are of importance in applications [6]. Planar polynomials  $\Pi$  and  $\Pi'$  with

$$\Pi' = (L_1 \circ \Pi \circ L_2)(x) + L_3(x)$$

are said to be *EA-equivalent* if  $L_1(x), L_2(x), L_3(x)$  are affine functions and  $L_1(x), L_2(x)$  are bijections [17]; and *linear equivalent* if  $L_1(x), L_2(x), L_3(x)$  are linear functions and  $L_1(x), L_2(x)$  are bijections. CCZ equivalence [6] is of interest in cryptographic applications. For planar Dembowski-Ostrom polynomials CCZ, EA and linear equivalence are equivalent [5].

Let

$$D_f(x, a) = f(x + a) - f(x) - f(a),$$

this is an alternate difference function to  $\Delta$  which is used to define planar functions [8].  $D_f(x, a)$  is more closely related to the semifield properties of planar functions. Another useful property of  $D$  is that for Dembowski-Ostrom polynomials

$$\Delta_{\Delta_{f,a},b}(x) = D_f(a, b).$$

**Observation 5** *Let  $f(x)$  be a DO polynomial on  $\mathbb{F}_{p^r}$ . Then  $f(x)$  is planar if and only if  $D_f(x, y) \neq 0$  for all  $x, y \in \mathbb{F}_{p^r}^*$ .*

**Theorem 6** *Let  $p$  be an odd prime and let*

$$f(x) = \text{Tr}(g(x)) + h(x) - (h(x))^{p^r}$$

*be a planar Dembowski-Ostrom polynomial in  $\mathbb{F}_{p^{2r}}$ . Let  $L_1(x), L_2(x), L_3(x)$  and  $L_4(x)$  be linear functions that are bijections on  $\mathbb{F}_{p^{2r}}$ .*

*If  $g'(x) = (L_1 \circ g \circ L_2)(x)$  and  $h'(x) = (L_3 \circ h \circ L_4)(x)$  then*

$$f'(x) = \text{Tr}(g'(x)) + h'(x) - (h'(x))^{p^r}$$

*is also a planar function.*

*Proof* The proof that  $f(x)$  is a planar function, Theorem 2, relies on showing that the sets

$$H = \{(a, b) \mid D_{Tr(g(x))}(a, b) = 0\}$$

and

$$K = \{(a, b) \mid D_{h(x)-(h(x))^{p^r}}(a, b) = 0\}$$

have no intersection for any  $a, b \in \mathbb{F}_{p^{2r}}$ .

Since  $L_1(x), L_3(x)$  are by definition permutations they have no roots other than zero [9, Lem 2.1]. Let

$$H' = \{(a, b) \mid D_{L_1 \circ Tr(g(x))}(a, b) = 0\}, \quad \text{then} \quad (9)$$

$$= \{(a, b) \mid L_1 \circ D_{Tr(g(x))}(a, b) = 0\} \quad (10)$$

$$= \{(a, b) \mid D_{Tr(g(x))}(a, b) = 0\} \quad (11)$$

$$= H. \quad (12)$$

Similarly

$$K' = \{(a, b) \mid D_{L_3(h(x)-(h(x))^{p^r})}(a, b) = 0\} = K,$$

hence  $L_1(x)$  and  $L_3(x)$  do not affect the planarity of  $f'(x)$ . Let

$$H'' = \{(a, b) \mid D_{Tr(g(L_2(x)))}(a, b) = 0\},$$

$$K'' = \{(a, b) \mid D_{h(L_4(x))-(h(L_4(x)))^{p^r}}(a, b) = 0\}.$$

Since  $L_2(x)$  and  $L_4(x)$  are permutations on  $x$ ,  $D_{Tr(g(L_2(x)))}(a, b) = D_{Tr(g(x))}(a, b)$  and  $D_{h(L_4(x))-(h(L_4(x)))^{p^r}}(a, b) = D_{h(x)-(h(x))^{p^r}}(a, b)$ . Thus  $H'' = H$  and  $K'' = K$  and  $L_2(x), L_4(x)$  have no effect on the planarity of  $f(x)$ .

Note that Theorem 6 includes the possibility that  $L_2(x) = L_4(x)$ , and  $L_1(x) = L_3(x)$ , in which case  $f(x)$  and  $f'(x)$  are CCZ-equivalent. However if  $L_1(x) \neq L_3(x)$  or  $L_2(x) \neq L_4(x)$  then  $f(x)$  and  $f'(x)$  are may be CCZ-nonequivalent.

### 3 Main Theorem

The main theorem of this paper is two new planar functions. These planar functions fit the shape of Theorem 2 Throughout this section  $p$  will be used to represent an odd prime power.

The following lemma is a statement of some of the facts from the proof of [9, Thm 3.3] and will be used in the proof of the main theorem.

**Lemma 7** *Let  $h(x) = x^{p^i+p^k} \in \mathbb{F}_{p^n}[x]$  with  $0 \leq i < k$ . Then the following are equivalent:*

- (i)  $h(x)$  is planar.
- (ii)  $D_h(x, a) \neq 0$  for all  $x, a \in \mathbb{F}_{p^n}^*$ ;
- (iii)  $z^{p^{k-i}-1} = -1$  has no solution in  $\mathbb{F}_{p^n}$ ;
- (iv)  $2 \nmid \frac{p^n - 1}{\gcd(p^n - 1, p^{k-i} - 1)}$ ;
- (v)  $\left| \langle b^{p^k-p^i} \rangle \right|$  is odd for any  $b \in \mathbb{F}_{p^n}^*$ .

We are now ready to prove the main theorem, which we restate for clarity.

*Proof (Proof of Theorem 1)* Since  $f_1(x)$  and  $f_2(x)$  are DO polynomials, by Observation 5,  $f_j(x)$  is planar if and only if  $D_{f_j}(x, a) \neq 0$  for all  $x, a \in \mathbb{F}_{p^{2r}}^*$ .

*Case 1.* Assume that  $f_1(x)$  is not planar. Then there exist elements  $x, a \in \mathbb{F}_{p^{2r}}^*$  such that  $D_{f_1}(x, a) = 0$ . Thus, from Theorem 2, there exists  $x, a \in \mathbb{F}_{p^{2r}}^*$  such that  $\text{Tr}(D_g(x, a)) = 0$  and  $D_h(x, a) \in \mathbb{F}_{p^r}$ . Since  $D_g(x, a) = 2xa$  and  $D_h(x, a) = x^{p^i}a^{p^k} + x^{p^k}a^{p^i}$ ,

$$2xa \left(1 + (2xa)^{p^r-1}\right) = 2xa + (2xa)^{p^r} = 0 \quad (13)$$

and

$$x^{p^i}a^{p^k} + x^{p^k}a^{p^i} \in \mathbb{F}_{p^r}. \quad (14)$$

Since  $x$  and  $a$  are invertible, Equation (13) implies that  $(2xa)^{p^r-1} = -1$  and therefore  $(xa)^{p^r-1} = -1$ .

Let  $\mathbb{F}_{p^r}^* \leq G \leq \mathbb{F}_{p^{2r}}^*$  such that  $|G| = 2|\mathbb{F}_{p^r}^*| = 2(p^r - 1)$ . Note that

$$G = \left\{ x \in \mathbb{F}_p^{2r} \mid x^{p^r-1} = \pm 1 \right\}.$$

Let  $c = xa$  then  $c \in G \setminus \mathbb{F}_{p^r}^*$ . From Equation (14)

$$\begin{aligned} x^{p^i}a^{p^k} + x^{p^k}a^{p^i} &= x^{p^i}a^{p^i} \left( a^{p^k-p^i} + x^{p^k-p^i} \right) \\ &= c^{p^i} \left( c^{p^k-p^i} x^{p^i-p^k} + x^{p^k-p^i} \right) \in \mathbb{F}_{p^r}. \end{aligned}$$

Since  $c \in G \setminus \mathbb{F}_{p^r}^*$ , the sum  $(c^{p^k-p^i} x^{p^i-p^k} + x^{p^k-p^i})$  is contained in  $G \setminus \mathbb{F}_{p^r}^*$ . By Lemma 7, both  $c^{p^k-p^i}$  and  $x^{p^k-p^i}$  are of odd order. Let  $\alpha \in \langle c^{p^k-p^i} \rangle$  such that  $\alpha^2 = c^{p^k-p^i}$ . Thus

$$\alpha \left( \alpha x^{p^i-p^k} + x^{p^k-p^i} \alpha^{-1} \right) = c^{p^k-p^i} x^{p^i-p^k} + x^{p^k-p^i} \in G \setminus \mathbb{F}_{p^r}^*.$$

Since  $\alpha \in G$  and  $|\langle \alpha \rangle|$  is odd,  $\alpha \in \mathbb{F}_{p^r}^*$ . Hence

$$\left( \alpha x^{p^i-p^k} + x^{p^k-p^i} \alpha^{-1} \right) \in G \setminus \mathbb{F}_{p^r}^*. \quad (15)$$

Let  $\omega = \alpha x^{p^i-p^k}$ . From (15),  $\omega + \omega^{-1} \in G \setminus \mathbb{F}_{p^r}^*$ ,  $\omega^2 + 2 + \omega^{-2} = (\omega + \omega^{-1})^2 \in \mathbb{F}_{p^r}^*$  and thus  $\omega^2 + \omega^{-2} \in \mathbb{F}_{p^r}$ . Since  $|\langle \omega \rangle|$  is odd and  $\omega + \omega^{-1} \in G \setminus \mathbb{F}_{p^r}^*$ , there exists an integer  $m > 1$  such that  $\omega^{2^m} + \omega^{-2^m} \in G \setminus \mathbb{F}_{p^r}^*$ . Let  $m$  be the minimal such integer. Then  $\omega^{2^{m-1}} + \omega^{-2^{m-1}} \in \mathbb{F}_{p^r}$  and

$$\begin{aligned} \omega^{2^m} + \omega^{-2^m} &= \omega^{2^m} + 2 + \omega^{-2^m} - 2 \\ &= \left( \omega^{2^{m-1}} + \omega^{-2^{m-1}} \right)^2 - 2 \\ &\in \mathbb{F}_{p^r} \end{aligned}$$

forming a contradiction. Hence there does not exist  $x, a \in \mathbb{F}_{p^{2r}}^*$  such that  $D_{f_1}(x, a) = 0$  and hence  $f_1(x)$  is a planar function.

*Case 2.* Assume that  $f_2(x)$  is not planar. Then there exist elements  $x, a \in \mathbb{F}_{p^{2r}}^*$  such that  $D_{f_2}(x, a) = 0$ . Thus, from Theorem 2,  $Tr(x^{p^i} a^{p^k} + x^{p^k} a^{p^i}) = Tr(D_h(x, a)) = 0$  and  $2xa = D_g(x, a) \in \mathbb{F}_{p^r}^*$ . By Lemma 7,  $x^{p^i} a^{p^k} + x^{p^k} a^{p^i} = D_h(x, a) \neq 0$ . Thus, since

$$(x^{p^i} a^{p^k} + x^{p^k} a^{p^i}) \left(1 + (x^{p^i} a^{p^k} + x^{p^k} a^{p^i})^{p^r-1}\right) = Tr(x^{p^i} a^{p^k} + x^{p^k} a^{p^i}) = 0,$$

$x^{p^i} a^{p^k} + x^{p^k} a^{p^i} \in G \setminus \mathbb{F}_{p^r}^*$ . Since

$$\begin{aligned} x^{p^i} a^{p^k} + x^{p^k} a^{p^i} &= x^{p^i} a^{p^i} (a^{p^k-p^i} + x^{p^k-p^i}) \\ &= c^{p^i} (c^{p^k-p^i} x^{p^i-p^k} + x^{p^k-p^i}) \in G \setminus \mathbb{F}_{p^r}^* \end{aligned}$$

where  $c = xa \in \mathbb{F}_{p^r}^*$ , the sum  $(c^{p^k-p^i} x^{p^i-p^k} + x^{p^k-p^i})$  is contained in  $G \setminus \mathbb{F}_{p^r}^*$ . Then using the same arguments as in the proof of case 1, there do not exist any elements  $c^{p^k-p^i}$  and  $x^{p^k-p^i}$  of odd order with  $c^{p^k-p^i} \in \mathbb{F}_{p^r}^*$  such that  $c^{p^k-p^i} x^{p^i-p^k} + x^{p^k-p^i} \in G \setminus \mathbb{F}_{p^r}^*$ . Hence, there do not exist elements  $x, a \in \mathbb{F}_{p^{2r}}^*$  with  $D_{f_2}(x, a) = 0$ , meaning  $f_2(x)$  is a planar function.

To see that  $f_1(x)$  and  $f_2(x)$  are not equivalent, note that when restricting to the subfield  $\mathbb{F}_{p^r}$

$$f_1(x)|_{\mathbb{F}_{p^r}} = 2g(x) \quad \text{and} \quad (16)$$

$$f_2(x)|_{\mathbb{F}_{p^r}} = 2h(x). \quad (17)$$

Hence, from [4, Prop 1],  $g(x)$  and  $h(x)$  are not equivalent.

Two families of planar functions have been constructed. In the next section it is shown that they are new. First we show that for specific fields, the family  $f_1$  contains several non-equivalent planar functions.

**Theorem 8** *Let  $u(x)$  and  $v(x)$  be two planar functions of type  $f_1(x)$  on  $\mathbb{F}_{p^r}$  with  $r$  odd and  $p \equiv 3 \pmod{4}$  such that*

$$u(x) = x^2 + x^{2p^r} + x^{1+p^k} - x^{(1+p^k)p^r}$$

$$v(x) = x^2 + x^{2p^r} + x^{1+p^j} - x^{(1+p^j)p^r}$$

*with  $j \neq k$ , then  $u(x)$  is not CCZ equivalent to  $v(x)$ .*

This proof is long and is separated into several Lemmas.

Let  $i^2 = -1$  then  $i \in \mathbb{F}_{p^{2r}} \setminus \mathbb{F}_{p^r}$ . Thus every element in  $\mathbb{F}_{p^{2r}}$  can be written uniquely as  $a + ib$  where  $a, b \in \mathbb{F}_{p^r}$ . Let  $\mathbb{F}_{p^2}^* \leq G \leq \mathbb{F}_{p^{2r}}^*$  be the unique subgroup with  $[G : \mathbb{F}_{p^r}^*] = 2$ . Assume that  $u(x) \equiv v(x)$  then there exist linear permutation polynomials

$$L_1(x) = \sum_{s=0}^{2r-1} c_s x^{p^s} \quad \text{and} \quad L_2(x) = \sum_{s=0}^{2r-1} d_s x^{p^s}$$

such that

$$(L_1 \circ f)(x) = (h \circ L_2)(x).$$

Let  $c_s = a_s + ib_s$  for some  $a_s, b_s \in \mathbb{F}_{p^r}$ .

Note that since  $p^r \equiv 3 \pmod{4}$  and  $j$  is even,  $(a_s + ib_s)^{p^r} = a_s - ib_s$  and  $(a_s + ib_s)^{p^j} = a_s^{p^j} + ib_s^{p^j}$ . Also note that the functions

$$(v \circ L_2)(x) + (v \circ L_2)(x)^{p^r} = \left( (2x^2 + 2x^{2p^r}) \circ L_2 \right)(x) \quad (18)$$

and

$$(v \circ L_2)(x) - (v \circ L_2)(x)^{p^r} = \left( (2x^{1+p^j} - 2x^{(1+p^j)p^r}) \circ L_2 \right)(x) \quad (19)$$

have terms whose exponents are of the form  $2p^s$  or  $(1+p^k)p^s$  only.

**Lemma 9** *For any  $0 \leq s < r$  one of the following is true:*

- 1)  $c_s = a_s$  and  $c_{s+r} = ib_{s+r}$ ;
- 2)  $c_s = ib_s$  and  $c_{s+r} = a_{s+r}$ ;
- 3)  $c_{s+r} = b_s + ia_s$ ;
- 4)  $c_{s+r} = -b_s - ia_s$ .

*Proof* From Equation (18) it follows that  $4c_s c_{s+r} + 4c_s^{p^r} c_{s+r}^{p^r} = 0$  (the coefficient of  $x^{(1+p^r)p^s}$ ). Thus  $c_s c_{s+r} \in G \setminus \mathbb{F}_{p^r} \cup \{0\}$ . But since

$$c_s c_{s+r} = (a_s + ib_s)(a_{s+r} + ib_{s+r}) \quad (20)$$

$$= (a_s a_{s+r} - b_s b_{s+r}) + i(a_s b_{s+r} + a_{s+r} b_s), \quad (21)$$

$$\Rightarrow a_s a_{s+r} = b_s b_{s+r}. \quad (22)$$

Furthermore, from Equation (18) it follows that  $2c_s^2 + 2c_{s+r}^{2p^r} = 2c_{s+r}^2 + 2c_s^{2p^r}$  (the coefficient of  $x^{2p^s}$  is equal to the coefficient of  $x^{2p^{s+r}}$ ). Thus  $c_s^2 + c_{s+r}^{2p^r} \in \mathbb{F}_{p^r}$ . But since

$$c_s^2 + c_{s+r}^{2p^r} = (a_s + ib_s)^2 + (a_{s+r} - ib_{s+r})^2 \quad (23)$$

$$= (a_s^2 - b_s^2 + a_{s+r}^2 + b_{s+r}^2) + i(2a_s b_s - 2a_{s+r} b_{s+r}), \quad (24)$$

$$\Rightarrow a_s b_s = a_{s+r} b_{s+r}. \quad (25)$$

From Equations (22) and (25), it follows that one of the following must hold:

- i.  $b_s = 0 = a_{s+r}$ ;
- ii.  $a_s = 0 = b_{s+r}$ ;
- iii.  $a_{s+r} = b_s$  and  $b_{s+r} = a_s$ ;
- iv.  $a_{s+r} = -b_s$  and  $b_{s+r} = -a_s$ .



**Lemma 10** *Let  $0 \leq s, t < 2r - 1$  such that  $t - s$  is even. If  $t - s$  is not equivalent to 0,  $k$ , or  $2r - k$  modulo  $2r - 1$  then one of the following must hold:*

- 1)  $c_s = 0 = c_{s+r}$ ;
- 2)  $c_t = 0 = c_{t+r}$ ;
- 3)  $c_{s+r} = b_s + ia_s$  and  $c_{t+r} = b_t + ia_t$ ;
- 4)  $c_{s+r} = -b_s - ia_s$  and  $c_{t+r} = -b_t - ia_t$ .

*Proof* From Equation (18) it follows that

$$4c_s c_t + 4c_{s+r}^{p^r} c_{t+r}^{p^r} = 0 \quad (26)$$

(the coefficient of  $x^{p^s + p^t}$ ). Likewise,

$$4c_s c_{t+r} + 4c_{s+r}^{p^r} c_t^{p^r} = 0 \quad (27)$$

(the coefficient of  $x^{p^s + p^{t+r}}$ ). From Equations (26) and (27) it follows that

$$(a_s a_t - b_s b_t) + i(b_s a_t + a_s b_t) = (-a_{s+r} a_{t+r} + b_{s+r} b_{t+r}) + i(b_{s+r} a_{t+r} + a_{s+r} b_{t+r}) \quad (28)$$

and

$$(a_s a_{t+r} - b_s b_{t+r}) + i(b_s a_{t+r} + a_s b_{t+r}) = (-a_{s+r} a_t + b_{s+r} b_t) + i(b_{s+r} a_t + a_{s+r} b_t). \quad (29)$$

From Lemma 9, there are four possible cases for the coefficients  $c_s$  and  $c_{s+r}$  and four possible cases for the coefficients  $c_t$  and  $c_{t+r}$  giving us a total of 16 cases. Suppose that we are in case (1) for  $c_s$ , and thus assume that  $b_s = 0 = a_{s+r}$ . Therefore, Equations (28) and (29) tell us that

$$\begin{aligned} a_s a_t &= b_{s+r} b_{t+r}, \\ a_s b_t &= b_{s+r} a_{t+r}, \\ a_s a_{t+r} &= b_{s+r} b_t, \\ \text{and } a_s b_{t+r} &= b_{s+r} a_t. \end{aligned}$$

It then follows that one of the following must hold:

- i.  $c_s = 0 = c_{s+r}$ ;
- ii.  $c_t = 0 = c_{t+r}$ ;
- iii.  $a_{s+r} = b_s$ ,  $b_{s+r} = a_s$ ,  $a_{t+r} = b_t$ , and  $b_{t+r} = a_t$ ;
- iv.  $a_{s+r} = -b_s$ ,  $b_{s+r} = -a_s$ ,  $a_{t+r} = -b_t$ , and  $b_{t+r} = -a_t$ .

A mirrored argument shows the same conclusion for the cases where  $c_s$  is in case (2) or  $c_t$  is in case (1) or (2) of Lemma 9.

Now suppose that we are in cases (3) or (4) of Lemma 9 for both pairs  $c_s, c_{s+r}$  and  $c_t, c_{t+r}$ . If both are in case (3) or both are in case (4) then we are done. Otherwise, let  $c_s$  be in case (3) and  $c_t$  be in case (4). Then Equation (28) becomes

$$(a_s a_t - b_s b_t) + i(b_s a_t + a_s b_t) = (b_s b_t - a_s a_t) - i(a_s b_t + b_s a_t).$$

Hence,  $a_s a_t = b_s b_t$  and  $a_s b_t = -b_s a_t$ . This then implies that  $b_s^2 = -a_s^2$ , alas  $b_s, a_s \in \mathbb{F}_{p^r}$ , so the only solution is  $b_s = a_s = 0$  and hence  $c_s = c_{s+r} = 0$ .

A mirrored argument shows that  $c_s$  in case (4) and  $c_t$  in case (3) yields  $c_t = c_{t+r} = 0$ .

**Lemma 11** *If either  $c_s$  or  $c_{s+r}$  is not zero then none of the following coefficients are zero:*

$$c_s, c_{s+r}, c_{s-j}, c_{s-j+r}, c_{s+j}, c_{s+j+r}.$$

Furthermore, either

- 1)  $c_{s+r} = b_s + ia_s$ ,  $c_{s-j+r} = b_{s-j} + ia_{s-j}$ , and  $c_{s+j+r} = b_{s+j} + ia_{s+j}$   
or
- 2)  $c_{s+r} = -b_s - ia_s$ ,  $c_{s-j+r} = -b_{s-j} - ia_{s-j}$  and  $c_{s+j+r} = -b_{s+j} - ia_{s+j}$ .

*Proof* From Equation (19) it follows that

$$2c_s c_s^{p^j} + 2c_{s+j} c_{s-j}^{p^j} - 2c_{s+r}^{p^r} c_{s+r}^{p^{j+r}} - 2c_{s+j+r}^{p^r} c_{s-j+r}^{p^{j+r}} = 0 \quad (30)$$

(the coefficient of  $x^{(1+p^j)p^s}$ ). Likewise,

$$2c_s c_{s+r}^{p^j} + 2c_{s+j+r} c_{s-j}^{p^j} - 2c_{s+r}^{p^r} c_s^{p^{j+r}} - 2c_{s+j}^{p^r} c_{s-j+r}^{p^{j+r}} = 0 \quad (31)$$

(the coefficient of  $x^{(1+p^{j+r})p^s}$ ). Since either  $c_s \neq 0$  or  $c_{s+r} \neq 0$ , by Lemma 10, there are three cases to handle.

Case 1.  $c_{s+j} = 0 = c_{s+j+r}$  and  $c_{s-j} = 0 = c_{s-j+r}$

Case 2.  $c_{s+r} = b_s + ia_s$ ,  $c_{s-j+r} = b_{s-j} + ia_{s-j}$ , and  $c_{s+j+r} = b_{s+j} + ia_{s+j}$

Case 3.  $c_{s+r} = -b_s - ia_s$ ,  $c_{s-j+r} = -b_{s-j} - ia_{s-j}$  and  $c_{s+j+r} = -b_{s+j} - ia_{s+j}$ .

In case 1, Equations (30) and (31) lead to  $a_s = 0$ ,  $b_s = 0$ ,  $a_{s+r} = 0$ , and  $b_{s+r} = 0$  forming a contradiction.

In cases 2 and 3, neither  $c_s$  nor  $c_{s+r}$  are zero. Plus, Equations (30) and (31) lead to the fact that  $c_{s+j}$  and  $c_{s-j}$  are not zero in order for  $c_s \neq 0$ .

*Proof (Proof of Theorem 8)* Suppose  $c_s \neq 0$ . By Lemma 11  $c_{s+j} \neq 0$ ,  $c_{s+2j} \neq 0$ , and  $c_{s+3j} \neq 0, \dots, c_{s-j} \neq 0$ . From Equation 19 it follows that

$$2c_s c_{s-j}^{p^j} - 2c_{s+r}^{p^r} c_{s-j+r}^{p^{r+j}} = 2c_{s+r} c_{s-j+r}^{p^j} - 2c_s^{p^r} c_{s-j}^{p^{r+j}}$$

(the coefficient of  $x^{2p^s}$  is equal to the coefficient of  $x^{2p^{s+r}}$ ). Thus

$$\left( c_s c_{s-j}^{p^j} - c_{s+r}^{p^r} c_{s-j+r}^{p^{r+j}} \right)^{p^r} = - \left( c_s c_{s-j}^{p^j} - c_{s+r}^{p^r} c_{s-j+r}^{p^{r+j}} \right)$$

and therefore  $c_s c_{s-j}^{p^j} - c_{s+r}^{p^r} c_{s-j+r}^{p^{r+j}} \in G \setminus \mathbb{F}_{p^r} \cup \{0\}$ . Since

$$\begin{aligned} & c_s c_{s-j}^{p^j} - c_{s+r}^{p^r} c_{s-j+r}^{p^{r+j}} \\ &= (a_s + ib_s)(a_{s-j}^{p^j} + ib_{s-j}^{p^j}) - (a_{s+r} - ib_{s+r})(a_{s-j+r}^{p^j} - ib_{s-j+r}^{p^j}) \\ &= (a_s + ib_s)(a_{s-j}^{p^j} + ib_{s-j}^{p^j}) - (\pm b_s \mp ia_s)(\pm b_{s-j}^{p^j} \mp ia_{s-j}^{p^j}) \\ &= (2a_s a_{s-j}^{p^j} - 2b_s b_{s-j}^{p^j}) \pm i(2b_s a_{s-j}^{p^j} + 2a_s b_{s-j}^{p^j}) \end{aligned}$$

is contained in  $G \setminus \mathbb{F}_{p^r} \cup \{0\}$ ,

$$a_s a_{s-j}^{p^j} = b_s b_{s-j}^{p^j}. \quad (32)$$

Furthermore, from Equation (19) it follows that

$$c_s c_{s-j+r}^{p^j} + c_{s+r} c_{s-j}^{p^j} - c_{s+r}^{p^r} c_{s-j}^{p^{j+r}} - c_s^{p^r} c_{s-j+r}^{p^{j+r}} = 0$$

(the coefficient of  $x^{(1+p^r)p^s}$ ). Thus

$$\left( c_s c_{s-j+r}^{p^j} + c_{s+r} c_{s-j}^{p^j} \right)^{p^r} = \left( c_s c_{s-j+r}^{p^j} + c_{s+r} c_{s-j}^{p^j} \right)$$

and therefore  $c_s c_{s-j+r}^{p^j} + c_{s+r} c_{s-j}^{p^j} \in \mathbb{F}_{p^r}$ . Since

$$\begin{aligned} c_s c_{s-j+r}^{p^j} + c_{s+r} c_{s-j}^{p^j} &= (a_s + i b_s)(\pm b_{s-j}^{p^j} \pm i a_{s-j}^{p^j}) + (\pm b_s \pm i a_s)(a_{s-j}^{p^j} + i b_{s-j}^{p^j}) \\ &= \pm(2a_s b_{s-j}^{p^j} - 2b_s a_{s-j}^{p^j}) \pm i(2a_s a_{s-j}^{p^j} + 2b_s b_{s-j}^{p^j}) \end{aligned}$$

is contained in  $\mathbb{F}_{p^r}$ ,

$$a_s a_{s-j}^{p^j} = -b_s b_{s-j}^{p^j}. \quad (33)$$

Since  $c_s \neq 0$  and  $c_{s-j} \neq 0$ , from Equations (32) and (33), it follows that either  $a_s = 0 = b_{s-j}$  or  $b_s = 0 = a_{s-j}$ . Hence, the coefficients  $c_s, c_{s+j}, c_{s+2j}, \dots, c_{s-j}$  alternate amongst the sets  $\mathbb{F}_{p^r}^*$  and  $G \setminus \mathbb{F}_{p^r}$ . But since  $r$  is odd and  $j$  is even, the set  $\{c_s, c_{s+j}, c_{s+2j}, \dots, c_{s-j}\}$  contains an odd number of coefficients. Therefore, it is impossible for the coefficients  $c_s, c_{s+j}, c_{s+2j}, \dots, c_{s-j}$  to all be nonzero and at the same time alternate amongst the sets  $\mathbb{F}_{p^r}^*$  and  $G \setminus \mathbb{F}_{p^r}$ . So by contradiction, there does not exist a nonzero coefficient  $c_s$ . Thus  $L_2(x) = 0$  and is not a permutation polynomial, and  $u(x)$  is not CCZ-equivalent to  $v(x)$ .

Theorem 1 shows two families of planar functions, and Theorem 8 shows that one of these families contains many CCZ-inequivalent planar functions. In the next section it is shown that these functions are in fact new.

#### 4 Non-equivalence with known functions

To determine if these planar functions are new, a check for CCZ-equivalence is required. There are seven families of planar functions that are on fields of any odd characteristic [2]. Each of these must be checked for equivalence with  $f_1(x)$  and  $f_2(x)$ . Note that if two functions are CCZ-equivalent, then they are CCZ-equivalent on any subfield.

Each of the proofs in this section make use of permutation polynomials

$$L_1(x) = \sum_{j=0}^{2r-1} c_j x^{p^j} \quad \text{and} \quad L_2(x) = \sum_{j=0}^{2r-1} d_j x^{p^j}.$$

**Lemma 12** *The functions  $f_1(x)$  and  $f_2(x)$  are not CCZ-equivalent to  $x^2$ .*

*Proof* Equation (17) shows that  $f_2(x)$  is not equivalent to  $x^2$ .

Assume that  $f_1$  is CCZ-equivalent to  $x^2$ . Note that since  $h(x) = x^{p^i(p^{k-i}+1)}$  is planar,  $k-i \not\equiv r \pmod{2r}$ . If  $f_1(x)$  is CCZ-equivalent to  $x^2$  then there exist permutation polynomials such that  $(L_1(x))^2 = L_2(f_1(x))$ . Note that

$$(L_1(x))^2 = \sum_{j=0}^{2r-1} c_j^2 x^{2p^j} + \sum_{0 \leq j < \ell < 2r} 2c_j c_\ell x^{p^j+p^\ell} \quad (34)$$

and

$$L_2(f_1(x)) = \sum_{j=0}^{r-1} (d_j + d_{j+r}) (x^{2p^j} + x^{2p^{j+r}}) + (d_j - d_{j+r}) (x^{(p^i+p^k)p^j} - x^{(p^i+p^k)p^{j+r}}).$$

Since  $k-i \not\equiv r \pmod{2r}$ ,  $2c_j c_{j+r} = 0$  for all  $0 \leq j < r$ . So for every  $0 \leq j < r$  either  $c_j = 0$  or  $c_{j+r} = 0$ . Furthermore,  $c_j^2 = (d_j + d_{j+r}) = c_{j+r}^2$  for all  $0 \leq j < r$ . Hence,  $c_j = c_{j+r} = 0$  for any  $0 \leq j < r$  and  $L_1(x) = 0$ . Since  $L_1(x)$  is not a permutation polynomial,  $f_1(x)$  is not CCZ-equivalent to  $x^2$ .

**Lemma 13** *The functions  $f_1(x)$  and  $f_2(x)$  are not equivalent to the planar functions derived from the Dickson semifields.*

*Proof* The planar functions derived from the Dickson semifields in  $\mathbb{F}_{p^{2r}}$  are [3]

$$d(x) = x^2 + \alpha \left( \frac{x^{p^r} - x}{\beta^{p^r} - \beta} \right)^{2p^m} - \beta^2 \left( \frac{x^{p^r} - x}{\beta^{p^r} - \beta} \right)^2$$

where  $\alpha$  is a non-square,  $\beta \in \mathbb{F}_{p^{2r}} \setminus \mathbb{F}_{p^r}$  and  $0 < m < 2r$ .

Note that  $d(x)|_{\mathbb{F}_{p^r}} = x^2$  and therefore  $f_2(x)$  is not CCZ-equivalent to  $d(x)$ .

Suppose that  $f_1(x)$  is equivalent to  $d(x)$ . Thus there exist linear permutation polynomials  $L_1(x), L_2(x) \in \mathbb{F}_{p^{2r}}[x]$  such that  $(f_1 \circ L_1)(x) = (L_2 \circ d)(x)$ . Note that

$$(L_2 \circ d)(x) = \sum_{j=0}^{2r-1} d_j \left( x^2 + \alpha \left( \frac{(x^{2p^r} - 2x^{p^r+1} + x^2)}{(\beta^{p^r} - \beta)^2} \right)^{p^m} - \beta^2 \left( \frac{(x^{2p^r} + x^{p^r+1} - x^2)}{(\beta^{p^r} - \beta)^2} \right) \right)^{p^j}.$$

Inspecting the various powers of  $x$  in  $(L_2 \circ d)(x)$  we find that only powers of the form  $2p^n$  or  $(p^{r+n} + p^n)$  for some  $0 \leq n < 2r$  are present.

*Case 1.* Suppose that there exists only one  $0 \leq s < r$  such that  $\{c_s, c_{s+r}\} \neq \{0\}$ . Then

$$\begin{aligned} (f_1 \circ L_1)(x) - (f_1 \circ L_1)(x)^{p^r} &= \\ &= 2 \left[ c_s^{p^k+p^i} x^{(p^k+p^i)p^s} + c_{s+r}^{p^k+p^i} x^{(p^k+p^i)p^{s+r}} + c_s^{p^k} c_{s+r}^{p^i} x^{(p^k+p^{i+r})p^s} \right. \\ &\quad + c_s^{p^i} c_{s+r}^{p^k} x^{(p^k+p^{i+r})p^{s+r}} - c_s^{(p^k+p^i)p^r} x^{(p^k+p^i)p^{s+r}} - c_{s+r}^{(p^k+p^i)p^r} x^{(p^k+p^i)p^s} \\ &\quad \left. - c_s^{p^k+r} c_{s+r}^{p^{i+r}} x^{(p^k+p^{i+r})p^{s+r}} - c_s^{p^{i+r}} c_{s+r}^{p^k+r} x^{(p^k+p^{i+r})p^s} \right]. \end{aligned} \quad (35)$$

Since none of the exponents of the terms in Equation (35) are of the form  $2p^n$  or  $(p^{r+n} + p^n)$ ,  $(f_1 \circ L_1)(x) - (f_1 \circ L_1)(x)^{p^r} = 0$ . Therefore, since  $L_1(x)$  is a permutation polynomial,  $f_1(x) - f_1(x)^{p^r} = 0$  forming a contradiction.

*Case 2.* Suppose that there exist at least two values  $0 \leq s < t < r$  such that  $\{c_s, c_{s+r}\} \neq \{0\}$  and  $\{c_t, c_{t+r}\} \neq \{0\}$ . Since the coefficients of  $x^{p^s+p^t}$  and  $x^{p^s+p^{t+r}}$  in  $(f_1 \circ L_1)(x) + (f_1 \circ L_1)(x)^{p^r}$  are  $4c_s c_t + 4c_{s+r}^p c_{t+r}^p$  and  $4c_s c_{t+r} + 4c_{s+r}^p c_t^p$  respectively,

$$c_s c_t + c_{s+r}^p c_{t+r}^p = 0 \quad (36)$$

and

$$c_s c_{t+r} + c_{s+r}^p c_t^p = 0.$$

Hence,  $c_s, c_{s+r}, c_t, c_{t+r} \in \mathbb{F}_{p^{2r}}^*$ . Now let  $a_s, a_t \in \mathbb{F}_{p^{2r}}^*$  such that  $c_{s+r}^p = a_s c_s$  and  $c_{t+r}^p = a_t c_t$ . From Equation (36),  $c_s c_t + a_s a_t c_s c_t = 0$  and therefore  $a_s a_t = -1$ . Likewise, if there exists a third value  $0 \leq \ell < r$  such that  $\{c_\ell, c_{\ell+r}\} \neq \{0\}$  then there exists  $a_\ell \in \mathbb{F}_{p^{2r}}^*$  such that  $a_s a_\ell = -1$ ,  $a_t a_\ell = -1$ , and  $a_s a_t = -1$ . Since this is not possible,  $c_s, c_{s+r}, c_t$  and  $c_{t+r}$  are the only non-zero coefficients of  $L_1(x)$ . Also note that if  $a_{s+r}, a_{t+r} \in \mathbb{F}_{p^{2r}}^*$  such that  $c_s^p = a_{s+r} c_{s+r}$  and  $c_t^p = a_{t+r} c_{t+r}$  then  $a_{s+r} a_t = -1$  and  $a_s a_{t+r} = -1$ . Hence,  $a_{s+r} = a_s$  and  $a_{t+r} = a_t$ .

Now note that

$$\begin{aligned} L_1(x)^{p^k+p^i} &= \\ &= (c_s x^{p^s} + c_t x^{p^t} + c_{s+r} x^{p^{s+r}} + c_{t+r}^p x^{p^{t+r}})^{p^k} (c_s x^{p^s} + c_t x^{p^t} + c_{s+r} x^{p^{s+r}} + c_{t+r}^p x^{p^{t+r}})^{p^i} \\ &= c_s^k c_s^i x^{(p^k+p^i)p^s} + c_{s+r}^k c_{s+r}^i x^{(p^k+p^i)p^{s+r}} + c_s^k c_{s+r}^i x^{(p^k+p^i)p^s+p^{s+r}} \\ &\quad + c_{s+r}^k c_s^i x^{(p^k+p^i)p^{s+r}+p^s} + c_t^k c_t^i x^{(p^k+p^i)p^t} + c_{t+r}^k c_{t+r}^i x^{(p^k+p^i)p^{t+r}} \\ &\quad + c_t^k c_{t+r}^i x^{(p^k+p^i)p^t+p^{t+r}} + c_{t+r}^k c_t^i x^{(p^k+p^i)p^{t+r}+p^t} + c_s^k c_t^i x^{(p^k+p^i)p^s+p^t} \\ &\quad + c_t^k c_{s+r}^i x^{(p^k+p^i)p^t+p^{s+r}} + c_{s+r}^k c_t^i x^{(p^k+p^i)p^{s+r}+p^t} + c_{s+r}^k c_{t+r}^i x^{(p^k+p^i)p^{s+r}+p^{t+r}} \\ &\quad + c_{t+r}^k c_{s+r}^i x^{(p^k+p^i)p^{t+r}+p^{s+r}} + c_s^k c_{s+r}^i x^{(p^k+p^i)p^s+p^{s+r}} \\ &\quad + c_{s+r}^k c_s^i x^{(p^k+p^i)p^{s+r}+p^s} + c_t^k c_{t+r}^i x^{(p^k+p^i)p^t+p^{t+r}} \\ &\quad + c_{t+r}^k c_t^i x^{(p^k+p^i)p^{t+r}+p^t} + c_s^k c_{t+r}^i x^{(p^k+p^i)p^s+p^{t+r}} \\ &\quad + c_{t+r}^k c_s^i x^{(p^k+p^i)p^{t+r}+p^s}. \end{aligned} \quad (37)$$

In order for  $(f_1 \circ L_1)(x) - (f_1 \circ L_1)(x)^{p^r} \neq 0$ , at least one of the terms in Equation (37) must have an exponent of the form  $2p^n$  or  $(p^{r+n} + p^n)$ . Thus  $s - t \in \{\pm(k - i), \pm(k - i) + r\}$ . Note that the only way for Equation (37) to be a sum of less than 16 terms is if  $s - t = t - s + r$ . But if this is true then  $2(s - t) = r$  and therefore  $2(k - i) = r$  forming a contradiction. Hence,  $L_1(x)^{p^k+p^i}$  is a sum of exactly 16 terms.

Since  $a_s a_t = -1$  and  $(f_1 \circ L_1)(x) - (f_1 \circ L_1)(x)^{p^r}$  only contains terms with exponents of the form  $2p^n$  or  $(p^{r+n} + p^n)$ ,

$$\begin{aligned}
(f_1 \circ L_1)(x) - (f_1 \circ L_1)(x)^{p^r} &= 2 \left[ L_1(x)^{p^k+p^i} - L_1(x)^{(p^k+p^i)p^r} \right] = \\
&= 2 \left( c_s^k c_t^i - c_{s+r}^{p^k+r} c_{t+r}^{p^i+r} \right) x^{(p^k+p^{i+t-s})p^s} + 2 \left( c_{s+r}^k c_{t+r}^i - c_s^{p^k+r} c_t^{p^i+r} \right) x^{(p^k+p^{i+t-s})p^{s+r}} \\
&+ 2 \left( c_s^k c_{t+r}^{p^i} - c_{s+r}^{p^k+r} c_t^{p^{i+r}} \right) x^{(p^k+p^{i+t-s+r})p^s} + 2 \left( c_{s+r}^k c_t^{p^i} - c_s^{p^k+r} c_{t+r}^{p^{i+r}} \right) x^{(p^k+p^{i+t-s+r})p^{s+r}} \\
&+ 2 \left( c_t^k c_s^i - c_{t+r}^{p^k+r} c_{s+r}^{p^i+r} \right) x^{(p^k+p^{i+s-t})p^t} + 2 \left( c_{t+r}^k c_{s+r}^i - c_t^{p^k+r} c_s^{p^{i+r}} \right) x^{(p^k+p^{i+s-t})p^{t+r}} \\
&+ 2 \left( c_t^k c_{s+r}^{p^i} - c_{t+r}^{p^k+r} c_s^{p^{i+r}} \right) x^{(p^k+p^{i+s-t+r})p^t} + 2 \left( c_{t+r}^k c_s^i - c_t^{p^k+r} c_{s+r}^{p^{i+r}} \right) x^{(p^k+p^{i+s-t+r})p^{t+r}} \\
&= 2 \left( 1 - a_s^k a_t^i \right) c_s^k c_t^i x^{(p^k+p^{i+t-s})p^s} + 2 \left( 1 - a_s^k a_t^i \right) c_{s+r}^k c_{t+r}^i x^{(p^k+p^{i+t-s})p^{s+r}} \\
&+ 2 \left( 1 - a_s^k a_t^i \right) c_s^k c_{t+r}^{p^i} x^{(p^k+p^{i+t-s+r})p^s} + 2 \left( 1 - a_s^k a_t^i \right) c_{s+r}^k c_t^{p^i} x^{(p^k+p^{i+t-s+r})p^{s+r}} \\
&+ 2 \left( 1 - a_t^k a_s^i \right) c_t^k c_s^i x^{(p^k+p^{i+s-t})p^t} + 2 \left( 1 - a_t^k a_s^i \right) c_{t+r}^k c_{s+r}^i x^{(p^k+p^{i+s-t})p^{t+r}} \\
&+ 2 \left( 1 - a_t^k a_s^i \right) c_t^k c_{s+r}^{p^i} x^{(p^k+p^{i+s-t+r})p^t} + 2 \left( 1 - a_t^k a_s^i \right) c_{t+r}^k c_s^i x^{(p^k+p^{i+s-t+r})p^{t+r}} \\
&= 2 \left( 1 + a_s^{p^k-i} \right) c_s^k c_t^i x^{(p^k+p^{i+t-s})p^s} + 2 \left( 1 + a_s^{p^k-i} \right) c_{s+r}^k c_{t+r}^i x^{(p^k+p^{i+t-s})p^{s+r}} \\
&+ 2 \left( 1 + a_s^{p^k-i} \right) c_s^k c_{t+r}^{p^i} x^{(p^k+p^{i+t-s+r})p^s} + 2 \left( 1 + a_s^{p^k-i} \right) c_{s+r}^k c_t^{p^i} x^{(p^k+p^{i+t-s+r})p^{s+r}} \\
&+ 2 \left( 1 + a_s^{p^i-k} \right) c_t^k c_s^i x^{(p^k+p^{i+s-t})p^t} + 2 \left( 1 + a_s^{p^i-k} \right) c_{t+r}^k c_{s+r}^i x^{(p^k+p^{i+s-t})p^{t+r}} \\
&+ 2 \left( 1 + a_s^{p^i-k} \right) c_t^k c_{s+r}^{p^i} x^{(p^k+p^{i+s-t+r})p^t} + 2 \left( 1 + a_s^{p^i-k} \right) c_{t+r}^k c_s^i x^{(p^k+p^{i+s-t+r})p^{t+r}}
\end{aligned} \tag{38}$$

Since  $1 + a_s^{p^i-k} = 0$  if and only if  $1 + a_s^{p^k-i} = 0$ , Equation (38) is either zero or a sum of exactly 8 terms. But it is impossible for all 8 of the terms to have exponents of the form  $2p^n$  or  $(p^{r+n} + p^n)$ . Hence,  $(f_1 \circ L_1)(x) - (f_1 \circ L_1)(x)^{p^r} = 0$  and thus  $f_1(x) - f_1(x)^{p^r} = 0$  forming a contradiction.

**Lemma 14** *The functions  $f_2(x)$  is not CCZ-equivalent to  $x^{p^m+1}$ . The function  $f_1(x)$  is not CCZ-equivalent to  $x^{p^m+1}$  on  $\mathbb{F}_{p^{2r}}$  where  $2r/\gcd(2r, m)$  odd.*

*Proof* Equation (16) shows that  $f_1(x)$  is not equivalent to  $x^{p^m+1}$ .

Assume that  $f_2(x)$  is CCZ-equivalent to  $x^{p^m+1}$ . Since  $h(x) = x^{p^i(p^{k-i}+1)} \in \mathbb{F}_{p^{2r}}[x]$  is planar,  $k-i \not\equiv r \pmod{2r}$ . If  $f_2(x)$  and  $x^{p^m+1}$  are CCZ-equivalent then there exist permutation polynomials  $L_1(x)$  and  $L_2(x)$  such that

$$(L_1(x))^{p^m+1} = L_2(f_2(x)).$$

Here

$$\begin{aligned} L_2(f_2(x)) &= \sum_{j=0}^{2r-1} d_j \left( x^{p^i+p^k} + \left( x^{p^i+p^k} \right)^{p^r} \right)^{p^j} + d_j \left( x^2 + x^{2p^r} \right)^{p^j} \\ &= \sum_{j=0}^{r-1} (d_j + d_{j+r}) \left( x^{(p^i+p^k)p^j} + x^{(p^i+p^k)p^{j+r}} \right) + (d_j - d_{j+r}) \left( x^{2p^j} - x^{2p^{j+r}} \right) \end{aligned}$$

and

$$\begin{aligned} (L_1(x))^{p^m+1} &= \left( \sum_{j=0}^{2r-1} c_j x^{p^j} \right)^{p^m+1} \\ &= \sum_{j=0}^{2r-1} c_j^{p^m+1} x^{p^j+p^{m+j}} + \sum_{0 \leq j < \ell < 2r} c_j c_\ell^{p^m} x^{p^j+p^{m+\ell}} \\ &\quad + \sum_{0 \leq j < \ell < 2r} c_j^{p^m} c_\ell x^{p^{m+j}+p^\ell}. \end{aligned} \quad (39)$$

Let

$$S_1 = \{p^j + p^{m+j} \pmod{p^{2r}-1} \mid j \in \mathbb{Z}, 0 \leq j < 2r\},$$

$$S_2 = \{p^j + p^{m+\ell} \pmod{p^{2r}-1} \mid j, \ell \in \mathbb{Z}, 0 \leq j < \ell < 2r\},$$

and

$$S_3 = \{p^{m+j} + p^\ell \pmod{p^{2r}-1} \mid j, \ell \in \mathbb{Z}, 0 \leq j < \ell < 2r\}.$$

Since  $m \not\equiv r \pmod{2r}$ ,  $|S_1| = 2r$  and  $|S_2| = |S_3| = \binom{2r}{2}$ . Moreover,  $|S_1 \cap S_2| = |S_1 \cap S_3| = |S_2 \cap S_3| = 0$ .

Since  $m \not\equiv r \pmod{2r}$ , for every  $0 \leq j < \ell < 2r$ , either  $j \not\equiv k-i+\ell \pmod{2r}$  or  $\ell \not\equiv k-i+j \pmod{2r}$  meaning either  $x^{p^j+p^{k-i+\ell}}$  or  $x^{p^\ell+p^{k-i+j}}$  is not CCZ-equivalent to  $x^2$ . Therefore, for all  $0 \leq j < \ell < 2r$ , either  $c_j c_\ell^{p^{k-i}} = 0$  or  $c_j^{p^{k-i}} c_\ell = 0$  and thus either  $c_j = 0$  or  $c_\ell = 0$ . So there exists at most one integer, say  $t$ , such that  $0 \leq t < 2r$  and  $c_t \neq 0$ . Hence,

$$\begin{aligned} &c_t^{p^m+1} x^{(p^m+1)p^t} \\ &= \sum_{j=0}^{r-1} (d_j + d_{j+r}) \left( x^{(p^i+p^k)p^j} + x^{(p^i+p^k)p^{j+r}} \right) + (d_j - d_{j+r}) \left( x^{2p^j} - x^{2p^{j+r}} \right). \end{aligned} \quad (40)$$

If  $k-1 \neq m$ , then Equation (40) has no solution and non-equivalence is shown. Assume  $k-i = m$ , then  $2(d_j - d_{j+r}) = 0$  for all  $0 \leq j < r$ , (the coefficient of  $x^{2p^j}$ ). This then implies that  $d_t = d_{t+r}$ . Next  $2(d_t + d_{t+r}) = c_t^{p^m+1}$ , (the coefficients of  $x^{(p^m+1)p^t}$ ), hence  $c_t^{p^m+1} = 4d_t$ . Rewriting Equation (40)

$$c_t^{p^m+1} x^{(p^m+1)p^t} = 4d_t (x^{(p^m+1)p^t} + x^{(p^m+1)p^{t+r}}) \quad (41)$$

we see that equality holds if and only if  $c_t = d_t = 0$ . Hence  $L_1(x)$  is not a permutation polynomial meaning  $f_2(x)$  is not CCZ-equivalent to  $x^{p^m+1}$ .

**Lemma 15** *The functions  $f_1(x)$  and  $f_2(x)$  are not CCZ-equivalent to*

$$f_{vi}(x) = x^{p^s+1} - a^{p^t-1}x^{p^{3t}+p^{t+s}}$$

over  $\mathbb{F}_{p^{4t}}$  where  $a \in \mathbb{F}_{p^{4t}} \setminus \mathbb{F}_{p^{2t}}$ ,  $p^s \equiv p^t \equiv 1 \pmod{4}$ , and  $2t/\gcd(s, 2t)$  is odd.

*Proof* Since  $f_1(x)$  and  $f_2(x)$  are planar over  $\mathbb{F}_{p^{2r}}$  for any  $r$ , whereas  $f_{vi}(x)$  requires  $r$  to be even with  $4t = 2r$ ,  $f_1(x)$  and  $f_2(x)$  are not equivalent to  $f_{vi}(x)$ .

**Theorem 16** *The function  $f_2(x)$  is not equivalent to any generalized Budaghyan-Helleseth function.*

The generalized Budaghyan-Helleseth planar functions on  $\mathbb{F}_{p^{2r}}$  are of the form

$$B(x) = x^{p^r+1} + \omega\beta x^{p^s+1} + \omega\beta^{p^r} x^{(p^s+1)p^r} \quad (42)$$

where  $\text{Tr}(\omega) = 0$ ,  $\beta^{p^r-1}$  is not in the subgroup of order  $(p^r+1)/\gcd(p^r+1, p^s+1)$ , and  $x^{p^s} \neq -x$  for all  $x \in \mathbb{F}_{p^{2r}}^*$ .

**Observation 17** *Note that the generalized Budaghyan-Helleseth functions can be written as*

$$B(x) = x^{p^r+1} + \omega\beta x^{p^s+1} - \left(\omega\beta x^{(p^s+1)}\right)^{p^r}$$

since  $\text{Tr}(\omega) = 0$ . Thus  $B(x) + B(x)^{p^r} = 2x^{p^r+1}$ .

*Proof (Proof of Theorem 16)* Suppose that  $f_2(x) \in \mathbb{F}_{p^{2r}}[x]$  is equivalent to a generalized Budaghyan-Helleseth function, thus there exist linear permutation polynomials  $L_1(x)$  and  $L_2(x)$  such that

$$B(L_1(x)) = L_2(f_2(x)).$$

Thus,

$$B(L_1(x)) + B(L_1(x))^{p^r} = L_2(f_2(x)) + L_2(f_2(x))^{p^r} \quad (43)$$

for any  $x \in \mathbb{F}_{p^{2r}}^*$ . By comparing the coefficients of  $x^{2p^n}$  for  $0 \leq n < r$  in Equation (43) it follows that

$$2c_n c_{n+r}^{p^r} = (d_n - d_{n+r}) - (d_n - d_{n+r})^{p^r} \in G \setminus \mathbb{F}_{p^r}^* \cup \{0\}$$

where  $\mathbb{F}_{p^r}^* \leq G \leq \mathbb{F}_{p^{2r}}^*$  is the unique subgroup with  $[G : \mathbb{F}_{p^r}^*] = 2$ . Let  $a_n = 2c_n c_{n+r}^{p^r} \in G \setminus \mathbb{F}_{p^r}^* \cup \{0\}$ .

Now by comparing the coefficients of  $x^{(p^r+1)p^n}$  for  $0 \leq n < r$  in Equation (43) it follows that

$$2c_n c_n^{p^r} + 2c_{n+r} c_{n+r}^{p^r} = 0.$$



Thus  $c_n = 0$  if and only if  $c_{n+r} = 0$ . Since  $L_1(x) \neq 0$ , there exists an integer  $0 \leq n < r$  such that  $c_n \neq 0$  and therefore  $a_n \neq 0$ .

$$2c_n c_n^{p^r} + 2c_{n+r} c_{n+r}^{p^r} = 0 \quad (44)$$

$$\implies 2c_n c_{n+r}^{p^r} \left(2c_n c_{n+r}^{p^r}\right)^{p^r} + \left(2c_{n+r} c_{n+r}^{p^r}\right)^2 = 0 \quad (45)$$

$$\implies a_n \cdot a_n^{p^r} + \left(2c_{n+r}^{p^r+1}\right)^2 = 0 \quad (46)$$

$$\implies -a_n^2 + \left(2c_{n+r}^{p^r+1}\right)^2 = 0 \quad \text{since } a_n \in G \setminus \mathbb{F}_{p^r}^* \quad (47)$$

$$\implies \left(2c_{n+r}^{p^r+1}\right)^2 = a_n^2 \quad (48)$$

$$\implies 2c_{n+r}^{p^r+1} = \pm a_n. \quad (49)$$

But  $2c_{n+r}^{p^r+1} \in \mathbb{F}_{p^r}^*$  and  $a_n \in G \setminus \mathbb{F}_{p^r}^*$ . Hence, by contradiction,  $f_2(x)$  is not equivalent to  $B(x)$ .

**Theorem 18** *If  $r$  is odd and  $p \equiv 3 \pmod{4}$  then  $f_1(x) \in \mathbb{F}_{p^{2r}}[x]$  is not equivalent to any generalized Budaghyan-Helleseth function.*

*Proof* Suppose that  $f_1(x) \in \mathbb{F}_{p^{2r}}[x]$  is equivalent to a generalized Budaghyan-Helleseth function. Thus, there exist linear permutation polynomials  $L_1(x)$  and  $L_2(x)$  such that

$$B(L_1(x)) = L_2(f_1(x)).$$

Therefore

$$B(L_1(x)) + B(L_1(x))^{p^r} = L_2(f_1(x)) + L_2(f_1(x))^{p^r} \quad (50)$$

for any  $x \in \mathbb{F}_{p^{2r}}$ . By comparing the coefficients of  $x^{2p^n}$  for  $0 \leq n < r$  in Equation (50) it follows that

$$2c_n c_{n+r}^{p^r} = \text{Tr}(d_n + d_{n+r}) \in \mathbb{F}_{p^r}.$$

Let  $a_n = 2c_n c_{n+r}^{p^r} \in \mathbb{F}_{p^r}$ .

By comparing the coefficients of  $x^{(p^r+1)p^n}$  for  $0 \leq n < r$  in Equation (50) it follows that

$$2c_n c_n^{p^r} + 2c_{n+r} c_{n+r}^{p^r} = 0.$$

Thus  $c_n = 0$  if and only if  $c_{n+r} = 0$ . Since  $L_1(x) \neq 0$ , there exists an integer  $0 \leq n < r$  such that  $c_n \neq 0$  and therefore  $a_n \neq 0$ . Then using the same arguments as Equations (44-49) it follow that

$$2c_{n+r}^{p^r+1} = \pm \sqrt{-1} a_n.$$

Since  $2c_{n+r}^{p^r+1} \in \mathbb{F}_{p^r}^*$  and  $a_n \in \mathbb{F}_{p^r}^*$ , it is required that  $\sqrt{-1} \in \mathbb{F}_{p^r}^*$ . But  $p \equiv 3 \pmod{4}$  and  $r$  is odd meaning  $\sqrt{-1} \notin \mathbb{F}_{p^r}^*$ . Hence, by contradiction,  $f_1(x)$  is not equivalent to  $B(x)$ .

**Theorem 19** *If either  $r$  is even or  $p \equiv 1 \pmod{4}$  then  $f_1(x) \in \mathbb{F}_{p^{2r}}[x]$  is equivalent to a generalized Budaghyan-Helleseth function.*

*Proof* Note that since either  $r$  is even or  $p \equiv 1 \pmod{4}$ ,  $\sqrt{-1} \in \mathbb{F}_{p^r}$  and thus  $\sqrt{-1}^{p^r} = \sqrt{-1}$ . Also note that since  $k-i$  is even,  $\sqrt{-1}^{p^k+p^i} = -1$  and  $\sqrt{-1}^{p^k} = \sqrt{-1}^{p^i}$ . Thus if  $L_1(x)$  is of the form  $c_0x + \sqrt{-1}c_0^{p^r}x^{p^r}$  then

$$f_1(L_1(x)) = 4\sqrt{-1}c_0^{p^r+1}x^{p^r+1} + 2c_0^{p^k+p^i}x^{p^k+p^i} - \left(2c_0^{p^k+p^i}x^{p^k+p^i}\right)^{p^r}.$$

*Case 1.* Suppose  $i = 0$ . Let  $L_1(x) = c_0x + \sqrt{-1}c_0^{p^r}x^{p^r}$  and  $L_2(x) = \frac{1}{4\sqrt{-1}c_0^{p^r+1}}x$ . Then

$$L_2(f_1(L_1(x))) = x^{p^r+1} + \frac{c_0^{p^k-p^r}}{2\sqrt{-1}}x^{p^k+1} - \left(\frac{c_0^{p^k-p^r}}{2\sqrt{-1}}x^{p^k+1}\right)^{p^r}.$$

*Case 2.* Suppose  $i = r$ . Let  $L_1(x) = c_0x + \sqrt{-1}c_0^{p^r}x^{p^r}$  and  $L_2(x) = \frac{1}{4\sqrt{-1}c_0^{p^r+1}}x^{p^r}$ . Then

$$L_2(f_1(L_1(x))) = x^{p^r+1} + \frac{c_0^{p^{k+r}-p^r}}{2\sqrt{-1}}x^{p^{k+r}+1} - \left(\frac{c_0^{p^{k+r}-p^r}}{2\sqrt{-1}}x^{p^{k+r}+1}\right)^{p^r}.$$

*Case 3.* Suppose  $i \notin \{0, r\}$ . Let  $L_1(x) = c_0x + \sqrt{-1}c_0^{p^r}x^{p^r}$  and  $L_2(x) = \frac{1}{8\sqrt{-1}c_0^{p^r+1}}x + \frac{1}{8\sqrt{-1}c_0^{p^r+1}}x^{p^r} + d_{2r-i}x^{p^{2r-i}} - d_{2r-i}x^{p^{r-i}}$  where  $d_{2r-i} \in \mathbb{F}_{p^r}$ . Then

$$L_2(f_1(L_1(x))) = x^{p^r+1} + 4c_0^{p^{k-i}+1}d_{2r-i}x^{p^{k-i}+1} - \left(4c_0^{p^{k-i}+1}d_{2r-i}x^{p^{k-i}+1}\right)^{p^r}.$$

**Lemma 20**  *$f_1(x)$  and  $f_2(x)$  are not equivalent to the Bierbrauer function (Theorem 4).*

*Proof* Inspection of the functions over the subfield  $\mathbb{F}_{p^r}$  shows that the Bierbrauer function is not equivalent to  $f_2(x)$ . Note that the Bierbrauer function is only planar when  $r$  is odd. From Theorem 8, the family  $f_1$  contains several nonequivalent planar functions on fields where  $r$  is odd,  $p \equiv 3 \pmod{4}$  and  $p^r > 3$ . Hence, on these fields at least some of the functions on family  $f_1$  are non-equivalent to the Bierbrauer function.

The following theorem then follows from Lemmas 12 through 20.

**Theorem 21** *If  $f_1(x), f_2(x) \in \mathbb{F}_{p^{2r}}[x]$  are as stated in Theorem 1 then*

- $f_1(x)$  is not equivalent to any known planar function over  $\mathbb{F}_{p^{2r}}$  when  $p \equiv 3 \pmod{4}$  and  $r$  is odd;
- $f_2(x)$  is not equivalent to any known planar function.

## 5 Other possible planar functions of the general form

This paper is concluded by some results that point out certain conditions that must hold amongst the polynomials  $g(x), h(x) \in \mathbb{F}_{p^{2r}}[x]$  in order for

$$f(x) = g(x) + (g(x))^{p^r} + h(x) - (h(x))^{p^r}$$

to be a planar function.

**Lemma 22** *The equality*

$$x^m + a^m = (x^n + a^n) \sum_{k=1}^{m/n} (-1)^{k+1} x^{m-kn} a^{(k-1)n}$$

holds if and only if  $n$  divides  $m$  and  $m/n$  is odd.

**Corollary 23** *Let  $g(x) = x^{p^i+p^j}$  and  $h(x) = x^{p^s+p^t}$  be polynomials on  $\mathbb{F}_{p^n}$  with  $i > j$  and  $s > t$ . Then  $D_g(x, a)$  divides  $D_h(x, a)$  if and only if  $i-j$  divides  $s-t$  and  $(s-t)/(i-j)$  is odd.*

**Theorem 24** *Let  $g(x), h(x) \in \mathbb{F}_{p^{2r}}[x]$  such that  $D_h(x, a) | D_g(x, a)$ . If  $g(x)$  is not a planar function then  $f(x)$  as described in Theorem 2 is not a planar function.*

*Proof* Because  $g(x)$  is not planar, there exist  $y, b \in \mathbb{F}_{p^{2r}}$  such that  $D_g(y, b) = 0$ . The divisibility conditions then implies that  $D_h(y, b) = 0$ . Hence  $D_f(y, b) = 0$  implying that  $f$  is not planar.

The conditions on divisibility given by Corollary 23 imply the following.

**Corollary 25** *Let  $g(x) = x^{p^i+p^j}$  and  $h(x) = x^{p^s+p^t}$  be polynomials on  $\mathbb{F}_{p^n}$  with  $i > j$  and  $s > t$  and  $(s-t)/(i-j)$  is an odd integer, then  $f(x)$  as described in Theorem 2 is not a planar function.*

**Theorem 26** *Let  $g(x), h(x) \in \mathbb{F}_{p^{2r}}[x]$ , with  $g(x) = x^{p^i+p^k}$  and  $h(x) = x^{p^s+p^t}$  where  $0 \leq i \leq k < 2r$  and  $0 \leq s \leq t < 2r$ . If  $f(x) = g(x) + (g(x))^{p^r} + h(x) - (h(x))^{p^r}$  then, depending on whether  $r, k-i$  and  $t-s$  are odd or even, the following table indicates when  $f(x)$  can possibly be planar.*

$r$	$k-i$	$t-s$	$f(x)$
Odd	Even	Odd	Not Planar
Odd	Odd	Odd	
Odd	Even	Even	Possibly Planar
Odd	Odd	Even	
Even	Even	Even	
Even	Even	Odd	
Even	Odd	Even	Not Planar
Even	Odd	Odd	

Namely, if  $f(x)$  is planar then either  $r$  is odd and  $t-s$  is even or  $r$  is even and  $k-i$  is even.

*Proof* Note that if  $f(x)$  is planar over  $\mathbb{F}_{p^{2r}}$  then it is also planar over the field  $\mathbb{F}_{p^2}$ . Here  $f(x)$  restricted to the subfield  $\mathbb{F}_{p^2}$  is:

$$f(x)|_{\mathbb{F}_{p^2}} = \begin{cases} x^2 + x^{2p} & \text{if } r \text{ is odd, } k-i \text{ is even and } t-s \text{ is odd;} \\ 2x^{p+1} & \text{if } r \text{ is odd, } k-i \text{ is odd and } t-s \text{ is odd;} \\ 2x^{p+1} \pm (x^2 - x^{2p}) & \text{if } r \text{ is odd, } k-i \text{ is odd and } t-s \text{ is even;} \\ 2x^{2p^{(1\pm 1)/2}} & \text{if } r \text{ is odd, } k-i \text{ is even and } t-s \text{ is even;} \\ 2x^{2p^{(1\pm 1)/2}} & \text{if } r \text{ is even, } k-i \text{ is even and } t-s \text{ is odd;} \\ 2x^{2p^{(1\pm 1)/2}} & \text{if } r \text{ is even, } k-i \text{ is even and } t-s \text{ is even;} \\ 2x^{p+1} & \text{if } r \text{ is even, } k-i \text{ is odd and } t-s \text{ is even;} \\ 2x^{p+1} & \text{if } r \text{ is even, } k-i \text{ is odd and } t-s \text{ is odd.} \end{cases}$$

However, over the field  $\mathbb{F}_{p^2}$ ,  $x^2 + x^{2p} = \text{Tr}(x^2)$  and is therefore not planar. Likewise, by [13], the monomial  $x^{p+1}$  is not planar over the field  $\mathbb{F}_{p^2}$ . Hence, if  $f(x)$  is planar then either  $r$  is odd and  $t-s$  is even or  $r$  is even and  $k-i$  is even.

Theorems 1 and 24 can then be summarized by the following theorem.

**Theorem 27** *Let*

$$f(x) = g(x) + (g(x))^{p^r} + h(x) - (h(x))^{p^r}$$

*with  $f(x), g(x), h(x) \in \mathbb{F}_{p^{2r}}[x]$ . Suppose  $g(x) = x^2$  and  $h(x)$  is a Dembowski-Ostrom polynomial. If  $f(x)$  is a planar polynomial, then  $h(x)$  is also a planar polynomial. If  $h(x)$  is a monomial, then  $f(x)$  is a planar polynomial if and only if  $h(x)$  is a planar monomial.*

## 6 Conclusion

Two new classes of planar functions have been demonstrated. Below is a new list of known planar functions which occur in fields of arbitrary odd characteristic, as updated from [2].

1.  $x^2$ ;
2. The planar functions derived from the Dickson semifields [10][3];
3.  $x^{m+1}$  on  $\mathbb{F}_{p^r}$  with  $r/\gcd(r, m)$  is odd [11];
4.  $x^{p^s+1} - a^{p^t-1}x^{p^{3t}+p^{t+s}}$  over  $\mathbb{F}_{p^{4t}}$  where  $a \in \mathbb{F}_{p^{4t}} \setminus \mathbb{F}_{p^{2t}}$ ,  $p^s \equiv p^t \equiv 1 \pmod{4}$ , and  $2t/\gcd(s, 2t)$  is odd [1];
5.  $x^{p^s+1} - a^{p^t-1}x^{p^t+p^{2t+s}}$  over  $\mathbb{F}_{p^{3t}}$  where  $a$  is primitive,  $\gcd(3, t) = 1$ ,  $t-s \equiv 0 \pmod{3}$ ,  $3t/\gcd(s, 3t)$  is odd [20];
6. The generalized Budaghyan-Helleseth functions [2][4];
7. The functions of Theorem 4, [2];
8.  $x^2 + x^{2p^r} + x^{(p^m+1)p^j} - x^{(p^m+1)p^{j+r}}$  over  $\mathbb{F}_{p^{2r}}$  where  $2r/\gcd(2r, m)$  is odd ( $f_1(x)$  of Theorem 1);
9. and  $x^{(p^m+1)p^j} + x^{(p^m+1)p^{j+r}} + x^2 - x^{2p^r}$  over  $\mathbb{F}_{p^{2r}}$  where  $2r/\gcd(2r, m)$  is odd ( $f_2(x)$  of Theorem 1).

In addition to the two new planar functions, a more general construction of planar functions has been shown on  $\mathbb{F}_{p^{2r}}$ . This construction method can be used to construct the two new functions as well as a recently discovered family of planar functions [2].

New planar functions are of theoretical and practical interest. Thus the construction method is of interest to generate new planar functions. There are many other possibilities for the seed functions of the construction. In particular, nothing as yet rules out the use of seed functions which are not Dembowski-Ostrom polynomials.

**Acknowledgements** Thanks to Asha Rao for helpful advice.

## References

1. Jürgen Bierbrauer. New semifields, PN and APN functions. *Designs, Codes and Cryptography*, 54:189–200, 2010. 10.1007/s10623-009-9318-7.
2. Jürgen Bierbrauer. Commutative semifields from projection mappings. *Designs, Codes and Cryptography*, 61:187–196, 2011. 10.1007/s10623-010-9447-z.
3. Lilya Budaghyan and Tor Helleseeth. New perfect nonlinear multinomials over  $\mathbb{F}_{p^{2k}}$  for any odd prime  $p$ . In Solomon Golomb, Matthew Parker, Alexander Pott, and Arne Winterhof, editors, *Sequences and Their Applications - SETA 2008*, volume 5203 of *Lecture Notes in Computer Science*, pages 403–414. Springer Berlin / Heidelberg, 2008.
4. Lilya Budaghyan and Tor Helleseeth. On isotopisms of commutative presemifields and ccz-equivalence of functions. *Int. J. Found. Comput. Sci.*, 22(6):1243–1258, 2011.
5. Lilya Budaghyan and Tor Helleseeth. New commutative semifields defined by new pn multinomials. *Cryptography and Communications*, 3:1–16, 2011.
6. Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Designs, Codes and Cryptography*, 15:125–156, 1998.
7. C. Carlet and C. Ding. Highly nonlinear mappings. *Journal of Complexity*, 20:205–244, 2004.
8. Robert S. Coulter and Marie Henderson. Commutative presemifields and semifields. *Advances in Mathematics*, 217(1):282 – 304, 2008.
9. R.S. Coulter and R.W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Designs, Codes and Cryptography*, 10(2):167–184, 1997.
10. L.E. Dickson. On commutative linear algebras in which division is always uniquely possible. *Transactions of the American Mathematical Society*, 7(4):514–522, 1906.
11. P. Dembowski and T.G. Ostrom. Planes of order  $n$  with collineation groups of order  $n^2$ . *Mathematische Zeitschrift*, 103(3):239–258, 1968.
12. C. Ding and J. Yin. Signal sets from functions with optimum nonlinearity. *Communications, IEEE Transactions on*, 55(5):936 –940, may 2007.
13. Tor Helleseeth, T. Rong and Daniel Sandberg. New families of almost perfect nonlinear power mappings. *IEEE Trans. Inf. Theory*, 8:475–485, 1999.
14. Tor Helleseeth and Daniel Sandberg. Some power mappings with low differential uniformity. *Applicable Algebra in Engineering, Communication and Computing*, 8:363–370, 1997.
15. K.J. Horadam. *Hadamard Matrices and Their Applications*. Princeton University Press, Princeton, New Jersey, 2007.
16. W. Jia, X. Zeng and T. Helleseeth. A class of binomial bent functions over the finite fields of odd characteristic. *IEEE Transactions on Information Theory*, 58(9): 6054–6063, 2012.
17. Gohar Kyureghyan and Alexander Pott. Some theorems on planar mappings. In Joachim von zur Gathen, Jos Imaai, and etin Ko, editors, *Arithmetic of Finite Fields*, volume 5130 of *Lecture Notes in Computer Science*, pages 117–122. Springer Berlin / Heidelberg, 2008.

- 
18. Alexander Pott and Yue Zhou. Switching construction of planar functions on finite fields. In M. Hasan and Tor Helleseth, editors, *Arithmetic of Finite Fields*, volume 6087 of *Lecture Notes in Computer Science*, pages 135–150. Springer Berlin / Heidelberg, 2010.
  19. A. Roy and A.J. Scott. Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements. *Journal of Mathematical Physics*, 48(072110):1–24, 2007.
  20. Zhengbang Zha, Gohar M. Kyureghyan, and Xueli Wang. Perfect nonlinear binomials and their semifields. *Finite Fields and Their Applications*, 15(2):125 – 133, 2009.